Eye on the Spy

Russell Buchan 2021-03-31T14:00:19

During the Covid-19 pandemic, more services and activities have migrated online. Digital supply chains have therefore emerged as the lifeblood of modern society and interferences with them can be hugely disruptive, as two recent incidents have illustrated.

In late 2020, SolarWinds, a US technology company, reported that its flagship Orion software had been hacked. The hack was 'likely Russian in origin' and involved the insertion of malware in Orion. Unwittingly, SolarWinds sent software updates to its customers containing the malware. Upon installation, the malware created a back door in customers' computer networks and systems that enabled third parties to covertly access their confidential data. While thousands of SolarWinds customers from across the world were affected, it was largely US users that fell victim to the hack and they included government agencies, Fortune 500 businesses and individual citizens.

In a separate incident, in early March 2021 Microsoft reported that a malicious actor – which it identified as a Chinese-run cyber espionage unit – had exploited flaws in its 2013, 2016 and 2019 Exchange Server email software, enabling unauthorised access to the email accounts of at least 30, 000 users worldwide, most of which were based in the US.

These hacks amounted to acts of cyber espionage insofar as they penetrated computer networks and systems in order to access and collect confidential data. In this post, I examine whether cyber espionage operations that can be attributed to a State under the law on State responsibility breach international law. This post addresses that question in two parts. First, I examine whether State-sponsored cyber espionage operations against digital supply chains infringe the principle of territorial sovereignty. Second, assuming that acts of cyber espionage *prima facie* breach the principle of territorial sovereignty, I consider whether States have carved out a permissive customary espionage 'exception' to it.

The Principle of Territorial Sovereignty

States have failed to devise international law that directly and specifically regulates peacetime espionage. This has led some commentators to conclude that international law is 'silent' on the practice of spying (Brown, 621). This approach is mistaken. As will be shown as this post progresses, espionage interacts with international law and there is an array of principles of general international law and specialised regimes that may apply to espionage operations depending upon the underlying act.

When it comes to hacks against digital supply chains, the most relevant rule of international law is the principle of territorial sovereignty. At its core, this principle

protects the exercise of inherently governmental functions from external interference. What qualifies as an inherently governmental function differs between governments depending on their political constitution. However, some functions can only be carried out by States, such as deciding who can enter and who can leave their territory.

According to the ICJ, acts of espionage breach the principle of territorial sovereignty where they involve non-consensual trespass into the physical territory of another State. Importantly, the territorial sovereignty principle applies to cyberspace but a thorny question is whether it prohibits remotely conducted cyber operations and, if so, under what circumstances. The Tallinn Manual experts agreed that the principle of territorial sovereignty applies to cyberspace and a majority of them held that it is only those State-sponsored cyber operations that produce harm against or within the cyber infrastructure of another State that breach this principle. More specifically, they concluded that it is only those remote cyber operations that, at a minimum, compromise the *functionality* of a computer system or network that are unlawful. Thus, the majority of experts determined that remotely launched cyber operations that merely intrude into the computer systems and networks of other States do not fall within the prohibitory scope of this principle. On the basis that remote access cyber espionage operations do not affect the functionality of computer networks or systems, these experts concluded that these operations do not fall foul of the principle of territorial sovereignty.

As Michael Schmitt observes, the approach adopted by the majority of the Tallinn Manual experts would mean that, as a cyber espionage operation, the SolarWinds hack would not transgress the principle of territorial sovereignty. Yet, Schmitt recognises that this position leaves digital supply chains vulnerable to espionage. He therefore *suggests* that, because the SolarWinds hack installed a back door in computer networks and systems and that operators had to patch this vulnerability in order to restore their integrity, it *could* be said that the hack caused sufficient damage to establish a breach of the principle of territorial sovereignty.

Schmitt's determination to interpret the principle of territorial sovereignty in such a way as to prohibit hacks against digital supply chains is commendable. By penetrating computer networks and systems in order to steal confidential data, cyber espionage operations can interfere with privacy-related rights, undermine trust and confidence in digital infrastructure, disrupt the delivery of essential services and, in extreme cases, threaten national security. International law must therefore prohibit cyber espionage and deter this activity. But the reality is that most hacks exploit vulnerabilities in computer networks or systems (after all, how was access obtained?) and require operators to take some type of remedial action, even if the patching process is quicker and easier for one-off, opportunistic hacks than it is for more sophisticated, intensive hacks that implant permanent back doors in networks or systems. Thus, Schmitt's approach would effectively mean that any non-consensual intrusion into confidential networks or systems would breach the principle of territorial sovereignty.

Perhaps it could be said that it is only those hacks that require *significant* remedial action on behalf of the system operator that violate the territorial sovereignty

principle. However, this approach is also beset with problems. In particular, it complexifies and subjectifies the application of the principle of territorial sovereignty, raising difficult questions as to which malicious cyber operations are sufficiently harmful to constitute a breach of this rule.

In my view, we must divorce the principle of territorial sovereignty from the requirement of harm or damage. We now live in a Digital Age. As the Tallinn Manual experts and the 2013 and 2015 UN GGEs concluded, States exercise sovereignty over the cyber infrastructure physically located within their territory and their sovereignty extends to the networks and systems that this infrastructure supports. If this is the case, why does a State's inherently governmental function to decide who enters its sovereign *physical* territory deserve more protection than its decision as to who enters its sovereign *cyber* infrastructure? There is no principled justification for this difference in approach. For me, the better view is that any non-consensual intrusion into computer networks or systems that are supported by cyber infrastructure that is physically located within the territory of another State amounts to a breach of the principle of territorial sovereignty, regardless of whether the targeted networks or systems are publicly or privately owned or operated. This approach also finds support in State practice (see France and Iran and, for a general discussion, see here). Importantly, this interpretation of the territorial sovereignty principle would prohibit remote access cyber espionage operations on the basis that they intrude into the victim State's sovereign cyber infrastructure by penetrating (without consent) computer networks and systems hosted by that infrastructure.

A Customary Espionage 'Exception'?

Some scholars concede that espionage *prima facie* breaches the principle of territorial sovereignty. Nevertheless, they argue that this principle contains an espionage 'exception' insofar as States have, through their practice, determined that acts of espionage (including cyber-enabled espionage) are not covered by this principle and are thus lawful. States are of course entitled to carve out exceptions to rules of international law but it goes without saying that they must be clearly established in State practice and *opinio juris*, the two essential elements of customary law.

State practice and *opinio juris* are difficult to identify in the context of espionage. There is no doubt that espionage is widely practised within the world order. Yet, espionage is an activity that is generally committed in secret. Critically, *secret* State practice is methodologically irrelevant to the formation of customary law (ILA, Principle 5). That said, it may be the case that the international community becomes aware of espionage via media reports, allegations by States or leaks by government employees. Does this constitute *public* State practice? For me, unless the impugned State admits involvement in espionage, leaks/allegations/reports do not amount to public State practice because, after all, the State neither endorses nor associates itself with that activity.

Additionally, State practice must be coupled with *opinio juris* for custom to form. O*pinio juris* is difficult to discern in the context of espionage because of the 'policy of silence' that surrounds this activity. Thus, very few States have justified espionage

as lawful under customary law. Admittedly, since the Snowden revelations some States have argued that espionage operations are lawful under international law, which may pave the way for a customary espionage exception to emerge. Yet, it is equally the case that, in response to the Snowden leaks, States such as Mexico condemned the US's cyber espionage as 'unacceptable, illegitimate and contrary to Mexican and international law'. I do not have space in this post to explore which States regard espionage as lawful or not. But what is clear is that *opinio juris* is too unsettled or even divergent to found a customary exception to a principle of general international law.

Conclusion

There is much hyperbole around the SolarWinds and Microsoft hacks. Rather than being destructive cyber attacks as some commentators (including Microsoft President Brad Smith) and US politicians (see here and here) have said, they were acts of cyber network exploitation and, to be fair, they are not unprecedented – their scale and sophistication is similar to cyber espionage operations carried out by other States in recent years. But international lawyers have worked themselves into a difficult position. Having previously averred that cyber espionage operations fall beyond the regulatory purview of international law, they now recognise the harm caused by such acts and have sought to cast them as destructive cyber attacks and do so in order to reach a different conclusion as to their legality under international law.

In my view, the better approach is to recognise that international law regulates espionage operations and, in particular, that it applies to the underlying act. In this post, I have argued for an interpretation of the principle of territorial sovereignty that prohibits cyber operations where they involve non-consensual trespass into a State's sovereign cyber infrastructure. Interpreted in this way, the territorial sovereignty principle provides States – and digital supply chains more generally – with powerful legal protection against cyber espionage.
